(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **10065662 A**

(43) Date of publication of application: **06 . 03 . 98**

(51) Int. Cl **H04L 9/08**
G11B 20/14
H04L 9/14
H04L 9/32
H04N 7/24

(21) Application number: **09082598**

(22) Date of filing: **01 . 04 . 97**

(30) Priority: **01 . 04 . 96 JP 08 78647**
10 . 06 . 96 JP 08147272

(71) Applicant: **SONY CORP**

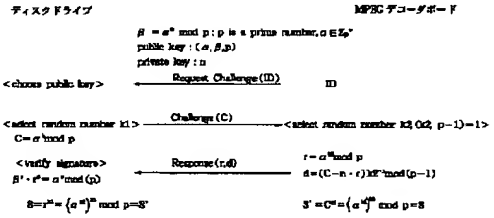
(72) Inventor: **ISHIGURO RYUJI**
OSAWA YOSHITOMO

(54) **DATA DECODING METHOD AND ITS DEVICE, AUTHENTICATING METHOD, RECORDING MEDIUM, DISK PRODUCING METHOD, RECORDING METHOD AND RECORDING DEVICE**

(57) Abstract:

PROBLEM TO BE SOLVED: To surely prevent illegal copying by ciphering reproduction data which is supplied to a decoder through the use of an undecipherable cipher key.

SOLUTION: When identification data transmitted from an MPEG decoder board and a public key corresponding to its ID are judged to be effective, a disk drive calculates Challenge (C) from an expression $C=\alpha k1 \bmod p$ and supplies it to the MPEG decoder board. In the expression, α and p are the public keys, p is prime number, and k1 is a properly selected random value. The MPEG decoder board selects the random value k2, calculates digital signature r and d and supplies them to the disk drive. The disk drive calculates β^r. γ^d, calculates $\alpha^c \bmod (p)$, judges whether or not the both values are equal and calculates Session key (S) in the care of being equal. In the meantime, the decoder board calculates Session key (S'). S becomes the value equal to S' and it means the same cipher key is obtained.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－65662

(43)公開日　平成10年(1998)３月６日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ	9/08			Ｈ０４Ｌ	9/00	６０１Ｃ
Ｇ１１Ｂ	20/14	３４１	9463－5D	Ｇ１１Ｂ	20/14	３４１Ｂ
Ｈ０４Ｌ	9/14			Ｈ０４Ｌ	9/00	６０１Ｅ
	9/32					６４１
Ｈ０４Ｎ	7/24					６７５Ａ

審査請求　未請求　請求項の数23　ＯＬ　（全 19 頁）　最終頁に続く

(21)出願番号　特願平9－82598

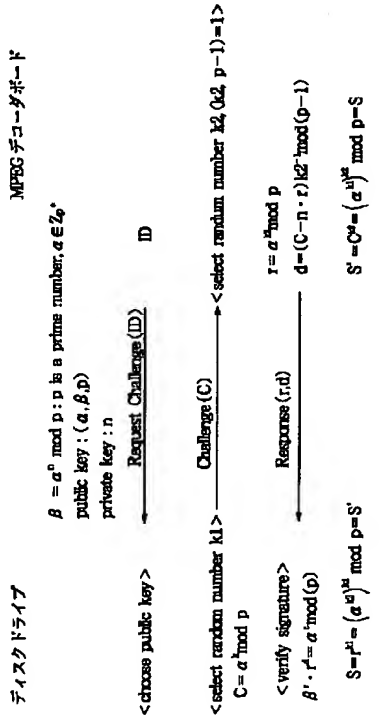
(22)出願日　平成９年(1997)４月１日

(31)優先権主張番号　特願平8－78647
(32)優先日　平８(1996)４月１日
(33)優先権主張国　日本（ＪＰ）
(31)優先権主張番号　特願平8－147272
(32)優先日　平８(1996)６月10日
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　石黒　隆二
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　大澤　義知
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　弁理士　稲本　義雄

(54)【発明の名称】　データ復号方法および装置、認証方法、記録媒体、ディスク製造方法、記録方法、並びに記録装置

(57)【要約】
【課題】　より安全な復号化方法を実現する。
【解決手段】　ＭＰＥＧデコーダボードは、メモリに記憶されているＩＤをディスクドライブに出力する。ディスクドライブは、ＤＶＤ－ＲＯＭに記憶されているキーテーブルからＩＤに対応する公開鍵を読み出し、この公開鍵を用いて、Ｃｈａｌｌｅｎｇｅ（Ｃ）を演算し、ＭＰＥＧデコーダボードに出力する。ＭＰＥＧデコーダボードは、Ｃｈａｌｌｅｎｇｅ（Ｃ）を用いて、デジタルシグニチャｒ，ｄを演算し、ディスクドライブに出力する。ディスクドライブは、デジタルシグニチャｒ，ｄを用いて、暗号化鍵を演算する。また、ＭＰＥＧデコーダボードは、Ｃｈａｌｌｅｎｇｅ（Ｃ）を用いて、暗号化鍵を演算する。



1

【特許請求の範囲】

【請求項１】　所定の暗号化鍵Ｓを用いてデータを暗号化することにより得られた暗号化データを第１の装置から受信し、その暗号化データを前記所定の暗号化鍵Ｓを用いて復号する第２の装置のデータ復号方法において、前記所定の暗号化鍵Ｓを用いて暗号化された暗号化データを前記第１の装置から受信するステップと、

所定の方法により生成された前記所定の暗号化鍵Ｓを用いて、前記暗号化データを復号するステップとを備え、前記所定の暗号化鍵Ｓを生成する前記所定の方法においては、

前記第１の装置と前記第２の装置のうちの一方が、前記第１の装置と前記第２の装置のうちの他方からの識別データを受信して、前記識別データに対応する公開鍵α，ｐを選択し、ランダム値ｋ１と前記公開鍵α，ｐから、

Ｃ＝αk1 mod ｐ

に従って第１のデータＣを演算し、その第１のデータＣを他方に供給し、

前記他方が、前記公開鍵α，ｐと、ランダム値ｋ２を用いて第２のデータｒを演算して、前記一方に供給するとともに、前記第１のデータＣと前記ランダム値ｋ２を用いて前記暗号化鍵Ｓを演算し、

さらに、前記一方が、前記他方から供給される前記第２のデータｒと前記ランダム値ｋ１を用いて前記暗号化鍵Ｓを演算することを特徴とするデータ復号方法。

【請求項２】　前記第１の装置と前記第２の装置との間で認証が行われ、前記認証においては、

前記他方が、前記第１のデータＣ、前記第２のデータｒ、前記公開鍵ｐ、前記ランダム値ｋ２および秘密鍵ｎを用いて、第３のデータｄを演算して、前記一方に供給し、

前記一方が、前記他方から供給される前記第２データｒと前記第３のデータｄと所定の公開鍵βとを用いて演算される値と、前記公開鍵α，ｐと前記第１のデータＣを用いて演算される値とを比較することを特徴とする請求項１に記載のデータ復号方法。

【請求項３】　前記データは暗号化鍵Ｑを用いて暗号化されたデータであり、

前記第２の装置は、前記暗号化鍵Ｓを用いて前記データを暗号化することにより得られた、暗号化データ及び前記暗号化された暗号化鍵ｘ，ｙを前記第１の装置から受信し、

前記所定の暗号化鍵Ｓを用いて前記暗号化データを復号して前記データを生成し、

前記暗号化された暗号化鍵ｘ，ｙを復号して復号された暗号化鍵Ｑを生成し、

その復号された暗号化鍵Ｑを用いて前記データを復号し、

前記暗号化された暗号化鍵ｘ、ｙは、前記暗号化鍵Ｑを前記公開鍵α，β，ｐを用いて暗号化することにより得られた鍵であり、

前記暗号化された暗号化鍵ｘ、ｙは、秘密鍵ｎ及び公開鍵ｐを用いて暗号化鍵Ｑに復号されることを特徴とする請求項２に記載のデータ復号方法。

【請求項４】　前記公開鍵α，ｐは記録媒体から再生されたデータであることを特徴とする請求項１に記載のデータ復号方法。

【請求項５】　所定の暗号化鍵Ｓを用いてデータを暗号化することにより得られた暗号化データを第１の装置から受信し、その暗号化データを前記所定の暗号化鍵Ｓを用いて復号するデータ復号装置において、

前記所定の暗号化鍵Ｓを用いて暗号化された暗号化データを前記第１の装置から受信する受信手段と、

前記所定の暗号化鍵Ｓを用いて、前記暗号化データを復号する第１の復号手段とを備え、

さらに、前記所定の暗号化鍵Ｓを生成するために、

前記第１の装置と前記復号装置のうちの一方が、前記第１の装置と前記復号装置のうちの他方からの識別データを受信して、前記識別データに対応する公開鍵α，ｐを選択し、ランダム値ｋ１と前記公開鍵α，ｐから、

Ｃ＝αk1 mod ｐ

に従って、第１のデータＣを演算し、その第１のデータＣを他方に供給する手段と、

前記他方が、前記公開鍵α，ｐと、ランダム値ｋ２を用いて第２のデータｒを演算して、前記一方に供給するとともに、前記第１のデータＣと前記ランダム値ｋ２を用いて前記暗号化鍵Ｓを演算する手段と、

さらに、前記一方が、前記他方から供給される前記第２のデータｒと前記ランダム値ｋ１を用いて前記暗号化鍵Ｓを演算する手段とを備えることを特徴とするデータ復号装置。

【請求項６】　前記第１の装置と前記データ復号装置との間で認証が行われ、前記認証のために、

前記他方が、前記第１のデータＣ、前記第２のデータｒ、前記公開鍵ｐ、前記ランダム値ｋ２および秘密鍵ｎを用いて、第３のデータｄを演算して、前記一方に供給する手段と、

前記一方が、前記他方から供給される前記第２のデータｒと前記第３のデータｄと所定の公開鍵βとを用いて演算される値と、前記公開鍵α，ｐと前記第１のデータＣを用いて演算される値とを比較する手段とを備えることを特徴とする請求項５に記載のデータ復号装置。

【請求項７】　前記データは暗号化鍵Ｑを用いて暗号化されたデータであり、

前記復号装置は、

前記暗号化鍵Ｓを用いて前記データを暗号化することにより得られた、暗号化データ及び前記暗号化された暗号化鍵ｘ，ｙを前記第１の装置から受信する受信手段と、

前記所定の暗号化鍵Ｓを用いて前記暗号化データを復号して前記データを生成する第１の復号手段と、

前記暗号化された暗号化鍵ｘ，ｙを復号して復号された暗号化鍵Ｑを生成する鍵復号手段と、
その復号された暗号化鍵Ｑを用いて前記データを復号する第２の復号手段とを有し、
前記暗号化された暗号化鍵ｘ、ｙは、前記暗号化鍵Ｑを前記公開鍵α，β，ｐを用いて暗号化することにより得られた鍵であり、
前記暗号化された暗号化鍵ｘ、ｙは、秘密鍵ｎ及び公開鍵ｐを用いて暗号化鍵Ｑに復号されることを特徴とする請求項５に記載のデータ復号装置。

【請求項８】　前記公開鍵α，ｐは記録媒体から再生されたデータであることを特徴とする請求項５に記載のデータ復号装置。

【請求項９】　所定の暗号化鍵Ｓを用いてデータを暗号化して、暗号化データを出力する第１の装置と、前記暗号化データを受信して、前記所定の暗号化鍵Ｓを用いて前記暗号化データを復号するデータ復号装置との間で、前記第１の装置と前記データ復号装置の一方が他方を認証する認証方法において、
前記第１の装置と前記データ復号装置のうちの一方が、前記第１の装置と前記データ復号装置のうちの他方からの識別データを受信して、前記識別データに対応する公開鍵α，ｐを選択し、ランダム値ｋ１と前記公開鍵α，ｐから、
Ｃ＝αk1 mod ｐ
に従って、第１のデータＣを演算し、その第１のデータＣを他方に供給するステップと、
前記他方が、前記公開鍵α，ｐと、ランダム値ｋ２を用いて第２のデータｒ，ｄを演算して、前記一方に供給するステップと、
前記一方が、前記他方から供給される前記第２のデータｒ，ｄと所定の公開鍵βとを用いて演算される値と、前記公開鍵α，ｐと前記第１のデータＣを用いて演算される値とを比較するステップとを備えることを特徴とする認証方法。

【請求項１０】　データを所定の暗号化鍵Ｓを用いて暗号化して、暗号化データを出力する第１の装置と、前記第１の装置からの前記暗号化データを前記暗号化鍵Ｓを用いて復号するデータ復号装置とにより構成される再生装置によって再生される記録媒体において、
前記記録媒体は記録データを含んでおり、前記記録データは、
前記暗号化鍵Ｓを演算するとき用いられる公開鍵α，ｐを前記第１の装置または前記データ復号装置を識別する識別データに対応させることにより、キーテーブルを生成するステップと、
前記データと前記キーテーブルを記録するステップから生成されていることを特徴とする記録媒体。

【請求項１１】　前記キーテーブルには、前記第１の装置または前記データ復号装置を識別するとき用いられる公開鍵βが、さらに、前記識別データに対応して含まれていることを特徴とする請求項１０に記載の記録媒体。

【請求項１２】　前記データは暗号化鍵Ｑにより暗号化されたデータであり、
前記キーテーブルには、前記暗号化鍵Ｑを前記公開鍵α，β，ｐを用いて暗号化した暗号化鍵ｘ，ｙが、さらに前記識別データに対応して含まれていることを特徴とする請求項１０に記載の記録媒体。

【請求項１３】　データを所定の暗号化鍵Ｓを用いて暗号化して、暗号化データを出力する第１の装置と、前記第１の装置からの前記暗号化データを前記暗号化鍵Ｓを用いて復号するデータ復号装置とにより構成される再生装置によって再生される記録媒体のための記録方法において、
前記暗号化鍵Ｓを演算するとき用いられる公開鍵α，ｐを前記第１の装置または前記データ復号装置を識別する識別データに対応させることにより、キーテーブルデータを生成するステップと、
前記データと前記キーテーブルを記録するステップとを備えることを特徴とする記録方法。

【請求項１４】　データを所定の暗号化鍵Ｓを用いて暗号化して、暗号化データを出力する第１の装置と、前記第１の装置からの前記暗号化データを前記暗号化鍵Ｓを用いて復号するデータ復号装置とにより構成される再生装置によって再生される記録媒体のための記録装置において、
前記暗号化鍵Ｓを演算するとき用いられる公開鍵α，ｐを前記第１の装置または前記データ復号装置を識別する識別データに対応させることにより、キーテーブルデータを生成する生成手段と、
前記データと前記キーテーブルを記録する記録手段とを備えることを特徴とする記録装置。

【請求項１５】　データを所定の暗号化鍵Ｓを用いて暗号化して、暗号化データを出力する第１の装置と、前記第１の装置からの前記暗号化データを前記暗号化鍵Ｓを用いて復号するデータ復号装置とにより構成される再生装置によって再生される記録媒体において、
前記記録媒体は記録データを含んでおり、前記記録データは、
前記第１の装置または前記データ復号装置を識別するとき用いられる公開鍵βを識別データに対応させることにより、キーテーブルを生成するステップと、
前記データと前記キーテーブルを記録するステップとから生成されていることを特徴とする記録媒体。

【請求項１６】　データを所定の暗号化鍵Ｓを用いて暗号化して、暗号化データを出力する第１の装置と、前記第１の装置からの前記暗号化データを前記暗号化鍵Ｓを用いて復号するデータ復号装置とにより構成される再生装置によって再生される記録媒体のための記録方法において、

前記第１の装置または前記データ復号装置を識別するとき用いられる公開鍵βを識別データに対応させることにより、キーテーブルデータを生成するステップと、
前記データと前記キーテーブルを記録するステップとを備えることを特徴とする記録方法。

【請求項１７】　データを所定の暗号化鍵Ｓを用いて暗号化して、暗号化データを出力する第１の装置と、前記第１の装置からの前記暗号化データを前記暗号化鍵Ｓを用いて復号するデータ復号装置とにより構成される再生装置によって再生される記録媒体のための記録装置において、
前記第１の装置または前記データ復号装置を識別するとき用いられる公開鍵βを識別データに対応させることにより、キーテーブルデータを生成する生成手段と、
前記データと前記キーテーブルを記録する記録手段とを備えることを特徴とする記録装置。

【請求項１８】　暗号鍵Ｑで暗号化されたデータを所定の暗号化鍵Ｓを用いて暗号化して、暗号化データを出力する第１の装置と、前記第１の装置からの前記暗号化データを前記暗号化鍵Ｓを用いて復号し、さらに、暗号化鍵Ｑを用いて復号するデータ復号装置とにより構成される再生装置によって再生される記録媒体において、
前記記録媒体は記録データを含んでおり、前記記録データは、
データを暗号化鍵Ｑで暗号化して、暗号化鍵Ｑで暗号化されたデータを生成するステップと、
前記暗号化鍵Ｑを、前記暗号化鍵Ｓを演算するとき用いられる公開鍵α，ｐと、前記第１の装置または前記データ復号装置を識別するとき用いられる公開鍵βとを用いて暗号化して得られた暗号化鍵ｘ，ｙを前記第１の装置または前記データ復号装置を識別する識別データに対応させることにより、キーテーブルを生成するステップと
前記暗号化鍵Ｑで暗号化されたデータと前記キーテーブルを記録するステップとから生成されていることを特徴とする記録媒体。

【請求項１９】　暗号鍵Ｑで暗号化されたデータを所定の暗号化鍵Ｓを用いて暗号化して、暗号化データを出力する第１の装置と、前記第１の装置からの前記暗号化データを前記暗号化鍵Ｓを用いて復号し、さらに、暗号化鍵Ｑを用いて復号するデータ復号装置とにより構成される再生装置によって再生される記録媒体のための記録方法において、
データを暗号化鍵Ｑで暗号化して、暗号化鍵Ｑで暗号化されたデータを生成するステップと、
前記暗号化鍵Ｑを、前記暗号化鍵Ｓを演算するとき用いられる公開鍵α，ｐと、前記第１の装置または前記データ復号装置を識別するとき用いられる公開鍵βとを用いて暗号化して得られた暗号化鍵ｘ，ｙを前記第１の装置または前記データ復号装置を識別する識別データに対応させることにより、キーテーブルを生成するステップと
前記暗号化鍵Ｑで暗号化されたデータと前記キーテーブルを記録するステップとを備えることを特徴とする記録方法。

【請求項２０】　暗号鍵Ｑで暗号化されたデータを所定の暗号化鍵Ｓを用いて暗号化して、暗号化データを出力する第１の装置と、前記第１の装置からの前記暗号化データを前記暗号化鍵Ｓを用いて復号し、さらに、暗号化鍵Ｑを用いて復号するデータ復号装置とにより構成される再生装置によって再生される記録媒体のための記録装置において、
データを暗号化鍵Ｑで暗号化して、暗号化鍵Ｑで暗号化されたデータを生成する暗号化手段と、
前記暗号化鍵Ｑを、前記暗号化鍵Ｓを演算するとき用いられる公開鍵α，ｐと、前記第１の装置または前記データ復号装置を識別するとき用いられる公開鍵βとを用いて暗号化して得られた暗号化鍵ｘ，ｙを前記第１の装置または前記データ復号装置を識別する識別データに対応させることにより、キーテーブルを生成する生成手段と
前記暗号化鍵Ｑで暗号化されたデータと前記キーテーブルを記録する記録手段とを備えることを特徴とする記録装置。

【請求項２１】　データを所定の暗号化鍵Ｓを用いて暗号化して、暗号化データを出力する第１の装置と、前記第１の装置からの前記暗号化データを前記暗号化鍵Ｓを用いて復号するデータ復号装置とにより構成される再生装置によって再生されるディスクを製造するためのディスク製造方法において、
前記暗号化鍵Ｓを演算するとき用いられる公開鍵α，ｐを前記第１の装置または前記データ復号装置を識別する識別データに対応させることにより、キーテーブルデータを生成するステップと、
前記データと前記キーテーブルを原盤に記録するステップと、
前記原盤から前記ディスクを生成するステップとを備えることを特徴とするディスク製造方法。

【請求項２２】　データを所定の暗号化鍵Ｓを用いて暗号化して、暗号化データを出力する第１の装置と、前記第１の装置からの前記暗号化データを前記暗号化鍵Ｓを用いて復号するデータ復号装置とにより構成される再生装置によって再生されるディスクを製造するためのディスク製造方法において、
前記第１の装置または前記データ復号装置を識別するとき用いられる公開鍵βを識別データに対応させることにより、キーテーブルデータを生成するステップと、
前記データと前記キーテーブルを原盤に記録するステップと、
前記原盤から前記ディスクを生成するステップとを備えることを特徴とするディスク製造方法。

【請求項２３】　暗号鍵Ｑで暗号化されたデータを所定の暗号化鍵Ｓを用いて暗号化して、暗号化データを出力

する第１の装置と、前記第１の装置からの前記暗号化データを前記暗号化鍵Ｓを用いて復号し、さらに、暗号化鍵Ｑを用いて復号するデータ復号装置とにより構成される再生装置によって再生されるディスクを製造するためのディスク製造方法において、

データを暗号化鍵Ｑで暗号化して、暗号化鍵Ｑで暗号化されたデータを生成するステップと、

前記暗号化鍵Ｑを、前記暗号化鍵Ｓを演算するとき用いられる公開鍵α，ｐと、前記第１の装置または前記データ復号装置を識別するとき用いられる公開鍵βとを用いて暗号化して得られた暗号化鍵ｘ，ｙを前記第１の装置または前記データ復号装置を識別する識別データに対応させることにより、キーテーブルを生成するステップと、

前記記暗号化鍵Ｑで暗号化されたデータと前記キーテーブルを原盤に記録するステップと、

前記原盤から前記ディスクを生成するステップとを備えることを特徴とするディスク製造方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、データ復号方法および装置、認証方法、記録媒体、ディスク製造方法、記録方法、並びに記録装置に関し、特に暗号化されているデータを、より安全に復号することができるようにした、データ復号化方法および装置、認証方法、記録媒体、ディスク製造方法、記録方法、並びに記録装置に関する。

【０００２】

【従来の技術】最近、デジタルビデオディスク（以下、ＤＶＤと記載する）のフォーマットが統一化されつつあり、統一化された場合、従来のアナログのビデオディスクに代わって普及することが期待されている。このＤＶＤにおいては、より長時間のビデオデータを記録することができるようにするために、ビデオデータが圧縮符号化（例えば、ＭＰＥＧ（Moving Picture Expert Group）方式、以下、ＭＰＥＧと記載し、MPEG方式を用いて説明する）されて記録される。従って、再生時においては、再生データを復号する必要がある。

【０００３】ところで、ＤＶＤにおいては、ビデオデータがデジタル的に記録されているため、これを他の記録媒体にコピーすると、ほとんどオリジナルのＤＶＤと遜色のない再生画像が得られる記録媒体を大量に複製することが可能となる。つまり、ディスクドライブとＭＰＥＧデコーダとの間でのデータの授受を盗聴され、この盗聴されたデータから不正のスタンパを生成することにより、不正のディスクが大量に複製されることになる。また、不正に製造されたＭＰＥＧデコーダを使用して、ディスクドライブからの再生データを復号し、この不正に復号された不正のスタンパを生成することにより、不正のディスクが大量に複製されることになる。

【０００４】このような不正コピーを防止したり、不正に製造されたＭＰＥＧデコーダを排除するために、ディスクドライブとＭＰＥＧデコーダとの間のデータとの授受において、正規のＭＰＥＧデコーダであるか否かを認証し、正規のＭＰＥＧデコーダであると認証された場合、ディスクドライブから再生データを暗号化鍵を用いて暗号化して、暗号化データをＭＰＥＧデコーダに供給する。そして、ＭＰＥＧデコーダは、この暗号化データを暗号化鍵を用いて復号（解読）し、さらに、復号（解読）された符号化データを復号するようにすることが考えられている。

【０００５】したがって、このような対策を取ることにより、不正に製造されたＭＰＥＧデコーダである場合は、ディスクドライブからの再生データがＭＰＥＧデコーダに供給されず、不正コピーを防止でき、かつ不正に製造されたＭＰＥＧデコーダを排除することができる。また、仮に正規のＭＰＥＧデコーダを装ってディスクドライブにアクセスされた場合、もしくはディスクドライブとＭＰＥＧデコーダとの間でのデータの授受を盗聴された場合に、ディスクドライブからの再生データを得られたとしても、その再生データは暗号化されているため、そのままではそのデータを用いることができない。従って、実質的なコピーを防止することができる。

【０００６】

【発明が解決しようとする課題】しかしながら、従来より提案されている単純な暗号化鍵を用いてＭＰＥＧデコーダに供給する再生データを暗号化し、ＭＰＥＧデコーダにおいて、その暗号化された再生データを復号する方法は、暗号化鍵が破られ易いという課題があった。

【０００７】本発明はこのような状況に鑑みてなされたものであり、本発明の目的は、デコーダに供給する再生データを破られ難い暗号化鍵を用いて暗号化することにより、不正コピーを確実に防止することができるようにすることにある。

【０００８】また、本発明の他の目的は、ディスクドライブからの再生データを暗号化する暗号化鍵の管理を容易にすることができるようにすることにある。

【０００９】

【課題を解決するための手段】請求項１に記載のデータ復号方法は、所定の暗号化鍵Ｓを用いて暗号化された暗号化データを第１の装置から受信するステップと、所定の方法により生成された所定の暗号化鍵Ｓを用いて、暗号化データを復号するステップとを備え、所定の暗号化鍵Ｓを生成する所定の方法においては、第１の装置と第２の装置のうちの一方が、第１の装置と第２の装置のうちの他方からの識別データを受信して、識別データに対応する公開鍵α，ｐを選択し、ランダム値ｋ１と公開鍵α，ｐから、Ｃ＝αk1 mod ｐに従って第１のデータＣを演算し、その第１のデータＣを他方に供給し、他方が、公開鍵α，ｐと、ランダム値ｋ２を用いて第２のデ

ータｒを演算して、一方に供給するとともに、第１のデータＣとランダム値ｋ２を用いて暗号化鍵Ｓを演算し、さらに、一方が、他方から供給される第２のデータｒとランダム値ｋ１を用いて暗号化鍵Ｓを演算することを特徴とする。

【００１０】請求項５に記載のデータ復号装置は、所定の暗号化鍵Ｓを用いて暗号化された暗号化データを第１の装置から受信する受信手段と、所定の暗号化鍵Ｓを用いて、暗号化データを復号する第１の復号手段とを備え、さらに、所定の暗号化鍵Ｓを生成するために、第１の装置と復号装置のうちの一方が、第１の装置と復号装置のうちの他方からの識別データを受信して、識別データに対応する公開鍵α，ｐを選択し、ランダム値ｋ１と公開鍵α，ｐから、Ｃ＝αk1 mod ｐに従って、第１のデータＣを演算し、その第１のデータＣを他方に供給する手段と、他方が、公開鍵α，ｐと、ランダム値ｋ２を用いて第２のデータｒを演算して、一方に供給するとともに、第１のデータＣとランダム値ｋ２を用いて暗号化鍵Ｓを演算する手段と、さらに、一方が、他方から供給される第２のデータｒとランダム値ｋ１を用いて暗号化鍵Ｓを演算する手段とを備えることを特徴とする。

【００１１】請求項９に記載の認証方法は、第１の装置とデータ復号装置のうちの一方が、第１の装置とデータ復号装置のうちの他方からの識別データを受信して、識別データに対応する公開鍵α，ｐを選択し、ランダム値ｋ１と公開鍵α，ｐから、Ｃ＝αk1 mod ｐに従って、第１のデータＣを演算し、その第１のデータＣを他方に供給するステップと、他方が、公開鍵α，ｐと、ランダム値ｋ２を用いて第２のデータｒ，ｄを演算して、一方に供給するステップと、一方が、他方から供給される第２のデータｒ，ｄと所定の公開鍵βとを用いて演算される値と、公開鍵α，ｐと第１のデータＣを用いて演算される値とを比較するステップとを備えることを特徴とする。

【００１２】請求項１０に記載の記録媒体は、記録媒体は記録データを含んでおり、記録データは、暗号化鍵Ｓを演算するとき用いられる公開鍵α，ｐを第１の装置またはデータ復号装置を識別する識別データに対応させることにより、キーテーブルを生成するステップと、データとキーテーブルを記録するステップから生成されていることを特徴とする。

【００１３】請求項１３に記載の記録方法は、暗号化鍵Ｓを演算するとき用いられる公開鍵α，ｐを第１の装置またはデータ復号装置を識別する識別データに対応させることにより、キーテーブルデータを生成するステップと、データとキーテーブルを記録するステップとを備えることを特徴とする。

【００１４】請求項１４に記載の記録装置は、暗号化鍵Ｓを演算するとき用いられる公開鍵α，ｐを第１の装置またはデータ復号装置を識別する識別データに対応させることにより、キーテーブルデータを生成する生成手段と、データとキーテーブルを記録する記録手段とを備えることを特徴とする。

【００１５】請求項１５に記載の記録媒体は、記録媒体は記録データを含んでおり、記録データは、第１の装置またはデータ復号装置を識別するとき用いられる公開鍵βを識別データに対応させることにより、キーテーブルを生成するステップと、データとキーテーブルを記録するステップとから生成されていることを特徴とする。

【００１６】請求項１６に記載の記録方法は、第１の装置またはデータ復号装置を識別するとき用いられる公開鍵βを識別データに対応させることにより、キーテーブルデータを生成するステップと、データとキーテーブルを記録するステップとを備えることを特徴とする。

【００１７】請求項１７に記載の記録装置は、第１の装置またはデータ復号装置を識別するとき用いられる公開鍵βを識別データに対応させることにより、キーテーブルデータを生成する生成手段と、データとキーテーブルを記録する記録手段とを備えることを特徴とする。

【００１８】請求項１８に記載の記録媒体は、記録媒体は記録データを含んでおり、記録データは、データを暗号化鍵Ｑで暗号化して、暗号化鍵Ｑで暗号化されたデータを生成するステップと、暗号化鍵Ｑを、暗号化鍵Ｓを演算するとき用いられる公開鍵α，ｐと、第１の装置またはデータ復号装置を識別するとき用いられる公開鍵βとを用いて暗号化して得られた暗号化鍵ｘ，ｙを第１の装置またはデータ復号装置を識別する識別データに対応させることにより、キーテーブルを生成するステップと暗号化鍵Ｑで暗号化されたデータとキーテーブルを記録するステップとから生成されていることを特徴とする。

【００１９】請求項１９に記載の記録方法は、データを暗号化鍵Ｑで暗号化して、暗号化鍵Ｑで暗号化されたデータを生成するステップと、暗号化鍵Ｑを、暗号化鍵Ｓを演算するとき用いられる公開鍵α，ｐと、第１の装置またはデータ復号装置を識別するとき用いられる公開鍵βとを用いて暗号化して得られた暗号化鍵ｘ，ｙを第１の装置またはデータ復号装置を識別する識別データに対応させることにより、キーテーブルを生成するステップと暗号化鍵Ｑで暗号化されたデータとキーテーブルを記録するステップとを備えることを特徴とする。

【００２０】請求項２０に記載の記録装置は、データを暗号化鍵Ｑで暗号化して、暗号化鍵Ｑで暗号化されたデータを生成する暗号化手段と、暗号化鍵Ｑを、暗号化鍵Ｓを演算するとき用いられる公開鍵α，ｐと、第１の装置またはデータ復号装置を識別するとき用いられる公開鍵βとを用いて暗号化して得られた暗号化鍵ｘ，ｙを第１の装置またはデータ復号装置を識別する識別データに対応させることにより、キーテーブルを生成する生成手段と暗号化鍵Ｑで暗号化されたデータとキーテーブルを記録する記録手段とを備えることを特徴とする。

【００２１】請求項２１に記載のディスク製造方法は、暗号化鍵Ｓを演算するとき用いられる公開鍵α，ｐを第１の装置またはデータ復号装置を識別する識別データに対応させることにより、キーテーブルデータを生成するステップと、データとキーテーブルを原盤に記録するステップと、原盤からディスクを生成するステップとを備えることを特徴とする。

【００２２】請求項２２に記載のディスク製造方法は、第１の装置またはデータ復号装置を識別するとき用いられる公開鍵βを識別データに対応させることにより、キーテーブルデータを生成するステップと、データとキーテーブルを原盤に記録するステップと、原盤からディスクを生成するステップとを備えることを特徴とする。

【００２３】請求項２３に記載のディスク製造方法は、データを暗号化鍵Ｑで暗号化して、暗号化鍵Ｑで暗号化されたデータを生成するステップと、暗号化鍵Ｑを、暗号化鍵Ｓを演算するとき用いられる公開鍵α，ｐと、第１の装置またはデータ復号装置を識別するとき用いられる公開鍵βとを用いて暗号化して得られた暗号化鍵ｘ，ｙを第１の装置またはデータ復号装置を識別する識別データに対応させることにより、キーテーブルを生成するステップと、記暗号化鍵Ｑで暗号化されたデータとキーテーブルを原盤に記録するステップと、原盤からディスクを生成するステップとを備えることを特徴とする。

【００２４】

【発明の実施の形態】図１は、本発明を適用した第１の実施の形態のパーソナルコンピュータの構成例を示している。この第１の実施の形態において、パーソナルコンピュータ１は、ＲＯＭタイプのディジタルビデオディスク（以下、ＤＶＤ－ＲＯＭと記載する）２を駆動するディスクドライブ１１と、ディスクドライブ１１によって再生された再生データが供給され、この再生データをデコードするＭＰＥＧデコーダボード１２とから構成されている。ＭＰＥＧデコーダボード１２からの復号された画像データ（以下、コンテンツデータ（Contents）と記載する）は、モニタ３に供給され、モニタ３は図示しない表示画面に再生画像を表示するようになされている。

【００２５】ディスクドライブ１１は、ＤＶＤ－ＲＯＭ２を駆動し、所定のアクセス点にアクセスすることにより、そこに記録されているデータを再生する駆動部２１、駆動部２１からの再生データを暗号化し、その暗号化データを出力する暗号化部２２、および、駆動部２１と暗号化部２２を制御する制御部２０から構成されている。ＤＶＤ－ＲＯＭ２には、所定の位置（例えば最内周トラック）に、暗号化に使用される公開鍵α，β，ｐを含むキーテーブルのデータが予め記録されている。なお。ＤＶＤ－ＲＯＭ２に記録されているコンテンツデータは、ＭＰＥＧ方式によって符号化されているデータである。

【００２６】また、ＭＰＥＧデコーダボード１２は、パーソナルコンピュータ１に対して、適宜装着されるボードであって、暗号化部２２より供給される暗号化データを復号（解読）し、復号（解読）された再生データを出力する復号部３１を有している。この復号部３１は、復号（解読）処理を行うのに必要な秘密鍵ｎと、ＭＰＥＧデコーダボード１２を識別するＩＤを記憶するメモリ３３を有している。

【００２７】復号部３１より出力された復号（解読）された再生データは、ＭＰＥＧデコード部３２に供給され、ＭＰＥＧデコード部３２は、ＭＰＥＧ方式に従って復号（解読）された再生データを復号し、コンテンツデータとして出力するようになされている。制御部３０は、復号部３１とＭＰＥＧデコード部３２を制御するようになされている。

【００２８】次に、図２と図３のフローチャート、図４のタイミングチャート及び図５の模式図を参照して、図１の第１の実施の形態の動作について説明する。なお、図２は、ディスクドライブ１１の動作を説明するためのフローチャートであり、図３は、ＭＰＥＧデコーダボード１２の動作を説明するフローチャートである。また、図４のタイミングチャートは、ディスクドライブ１１とＭＰＥＧデコーダボード１２との間において授受されるデータと、各データに対応して実行される演算を表している。さらに、図５は、ディスクドライブ１１とＭＰＥＧデコーダボード８２との間でのデータの流れを示すための模式図である。

【００２９】ＤＶＤ－ＲＯＭ２に記録されているデータを再生する場合、最初に、図３のステップＳ２１において、ＭＰＥＧデコーダボード１２の制御部３０は、ＭＰＥＧデコーダボード１２の識別データとしてのＩＤを復号部３１のメモリ３３から読み出し、ディスクドライブ１１の制御部２０に送信する。このＩＤは、図４に示すように、Request Challenge（ＩＤ）として、ディスクドライブ１１に送られる。

【００３０】図２のステップＳ１において、ディスクドライブ１１の制御部２０は、ＭＰＥＧデコーダボード１２の制御部３０から送られてきたＩＤを受け取る。そして、制御部２０はステップＳ２に進み、ステップＳ１で受け取ったＩＤに対応する公開鍵を、ＤＶＤ－ＲＯＭ２から読み取るように、駆動部２０を制御する。

【００３１】すなわち、図５に模式的に示すように、ＤＶＤ－ＲＯＭ２の所定のトラックには、キーテーブルとして、このＤＶＤ－ＲＯＭ２を再生して得られるＭＰＥＧ方式によって符号化されているコンテンツデータを暗号化する複数の公開鍵（public key）が、各公開鍵（ｋｅｙ１，ｋｅｙ２，ｋｅｙ３，・・・）が有効であるか否かを表すフラグと共に記録されている。図５において、有効な公開鍵（ｋｅｙ１，ｋｅｙ２）は○印を付して表し、無効な公開鍵（ｋｅｙ３）は×印を付して表している。ＤＶＤ－ＲＯＭ２を初めて製造したとき、全て

の公開鍵は有効とされている。しかしながら、例えば、公開鍵の中の所定のもの（図５の第１の実施の形態の場合、ｋｅｙ３）が第３者に破られてしまったような場合、その公開鍵に対応するフラグは、以後、無効として記録される。

【００３２】なお、各公開鍵ｋｅｙ１，ｋｅｙ２，ｋｅｙ３，・・・は、それぞれ公開鍵（α１，β１，ｐ１），（α２，β２，ｐ２），（α３，β３，ｐ３），・・・で構成される。

【００３３】このような公開鍵と有効フラグを表すキーテーブルが、ＤＶＤ－ＲＯＭ２のＲＯＭ領域に記録されている場合においては、これを書き換えることができないため、新しいバージョンのディスクとして、実質的に同一のコンテンツデータが記録されているディスクを新たに製造するとき、キーテーブルの有効フラグだけが書き換えられる。

【００３４】制御部２０は、駆動部２１を制御し、駆動部２１は、ＤＶＤ－ＲＯＭ２の所定のトラックに記録されているキーテーブルを読み出す。そして、この読み出したキーテーブルは制御部２０に供給され、制御部２０は、この読み出されたキーテーブルから、ステップＳ１で受け取ったＩＤに対応する公開鍵及びその公開鍵に対応するフラグを検出する。換言すれば、ＭＰＥＧデコーダボード１２の正規の製造者に対してはＩＤが予め与えられており、ＤＶＤ－ＲＯＭ２の製造者は、各ＩＤに対応する公開鍵を選定し、テーブルに記憶しておく。そこで、このステップＳ２で、各ＩＤに対応する公開鍵及びフラグが検出される。

【００３５】さらに、ステップＳ３において、制御部２０は、その公開鍵に対応するフラグが有効とされているか否かを判定する。上述したように、例えば、不正コピーを行っているＭＰＥＧデコーダボード１２の製造者（ボードメーカー）に割り当てられているＩＤが発見された場合においては、そのＩＤに対応する公開鍵は無効とされる。そして、その発見後に製造されるＤＶＤ－ＲＯＭ２には、その公開鍵を無効とするフラグが記録される。ステップＳ１で受け取ったＩＤに対応する公開鍵が無効と判定された場合、処理が終了される。すなわち、この場合においては、ＭＰＥＧデコーダボード１２は、ＤＶＤ－ＲＯＭ２の再生データを受け取ることができないことになる。

【００３６】一方、ステップ３において、ステップＳ１で受け取ったＩＤに対応する公開鍵が有効であると判定された場合、ステップＳ４に進み、制御部２０は、次式（１）からChallenge（Ｃ）を計算し、図４に示すように、このChallenge（Ｃ）としてＭＰＥＧデコーダボード１２の制御部３０に供給する。

$C=\alpha^{k1} \bmod p \cdots (1)$

【００３７】ここで、α，ｐは、ＤＶＤ－ＲＯＭ２のキーテーブルに記録されている公開鍵であり、ｐは素数である。また、ｋ１は、適宜選択されるランダムな番号（値）である。また、Ａ mod Ｂは、ＡをＢで割算したとき得られる剰余を表している。

【００３８】上述した式（１）は、トラップドアファンクションの関数（離散対数問題）として知られており、ｋ１からＣは容易に計算できるが、Ｃからｋ１を計算することができる関数は知られていない。

【００３９】図４に示すように、このようにして計算されたChallenge（Ｃ）は、ＭＰＥＧデコーダボード１２の制御部３０に供給される。制御部３０は、図３のステップＳ２２において、このChallenge（Ｃ）を受け取る。そして、制御部３０は、ステップＳ２３に進み、所定のランダムな番号ｋ２を選択し、次式（２）、（３）からデジタルシグニチャｒ，ｄを演算し、その結果をResponse（ｒ，ｄ）として、ディスクドライブ１１に供給する。

$r=\alpha^{k2} \bmod p \quad \cdots (2)$

$d=(C-n\cdot r)\, k2^{-1} \bmod (p-1) \cdots (3)$

【００４０】なお、このランダムな値ｋ２は、ｐ－１と素の関係にある。

【００４１】図４に示すように、上述した式（２）及び（３）から求められたデジタルシグニチャｒ，ｄは、Response（ｒ，ｄ）として、ディスクドライブ１１の制御回路２０に供給される。制御部２０は、図２のステップＳ５において、このResponse（ｒ，ｄ）を受け取り、ステップＳ６に進み、ステップ６において、このResponse（ｒ，ｄ）内のデジタルシグニチャｒ，ｄをチェックする。

【００４２】すなわち、制御部２０は、図４に示すように、βｒ・ｒｄを演算するとともに、αC mod （ｐ）を演算し、両者の値が等しいか否かを判定する。ＭＰＥＧデコーダボード１２が、正規のデコーダである場合、デジタルシグニチャｒ，ｄと公開鍵βとを用いて演算される値βｒ・ｒｄの値は、Challenge（Ｃ）、公開鍵α，ｐを用いて求められる値αC mod （ｐ）の値と等しくなる。この２つの演算値が等しくなることは、ＥｌＧａｍａｌ Ｓｉｇｎａｔｕｒｅ Ｓｃｈｅｍｅとして、よく知られている（A public key cryptosystem and a signature scheme basedon discrete logarithms. IEEE Transactions on Information Theory, 21 (1985),469-472）。逆に、ＭＰＥＧデコーダボード１２が正規の デコーダではない場合、両者の値は異なるものとなる。この場合、処理は終了される。従って、この場合、ＤＶＤ－ＲＯＭ２の再生データはＭＰＥＧデコーダボード１２に出力されないことになる。なお、ここまでのデータの授受の流れが、図５に示されるKey Exchangeに対応している。

【００４３】ステップＳ６において、演算された２つの値が等しいと判定された場合、ステップＳ７に進み、制御部２０は、Session key (S) を次式（４）より演算す

る（図５のSession Key S）。

S＝rk1…（４）

【００４４】一方、ＭＰＥＧデコーダボード１２の制御部３０は、図３のステップＳ２３において、Response（r，d）を計算して、ディスクドライブ１１に供給した後、ステップＳ２４に進み、ステップＳ２２で受け取ったChallenge（C）を用いて次式（５）に従って、Session key（S*）を演算する（図５のSession Key S*）。

S’＝Ck2　…（５）

【００４５】図２のフローチャートのステップＳ７において、ディスクドライブ１１の制御部２０によって計算されたSession KeyＳと、図３のフローチャートのステップＳ２４においてＭＰＥＧデコーダボード１２の制御部３０によって演算されたSession KeyＳ’は、それぞれ次式（６）及び（７）で表され、両者は等しい値となる。すなわち、ディスクドライブ１１とＭＰＥＧデコーダボード１２において、それぞれ同一の暗号化鍵が得られたことになる。

S＝rk1＝（αk2）k1 mod p　…（６）

S’＝Ck2＝（αk1）k2 mod p　…（７）

【００４６】このことは、Diffie－Hellmen Key Exchangeにおいて知られている（Diffie-Hellman W. Diffie and M. E. Hellman. Multiuser cryptographic techniques. A FIPS Conference Proceedings, 45(1976), 102-112）。

【００４７】そこで、ディスクドライブ１１の制御部２０は、ステップＳ８に進み、駆動部２１にＤＶＤ－ＲＯＭ２を駆動させるとともに、ステップＳ７で求めたSessionKey Ｓを暗号化部２２に供給する。そして、駆動部２１は、ＤＶＤ－ＲＯＭ２の所定の位置から記録されているデータを再生する。暗号化部２２は、駆動部２１でＤＶＤ－ＲＯＭ２から再生された再生データをステップＳ７で求めたSessionKey Ｓを用いて暗号化して、暗号化データを生成する。そして、この暗号化データは、ＭＰＥＧデコーダボード１２に供給される（図５のEncryption）。

【００４８】ＭＰＥＧデコーダボード１２の復号部３１は、図３のステップＳ２５で、暗号化部２２から供給された暗号化データを受け取り、ステップＳ２６において、その暗号化データを、ステップＳ２４で求めたSession Key Ｓ’を用いて復号（解読）する（図５のDecryption）。上述したように、Session Key Ｓ’は、セッションキーＳと同一の値であるので、正しい復号（暗号の解読）を行うことができる。そして、この復号（解読）された再生データ（符号化されているコンテンツデータ）がＭＰＥＧデコード部３２供給される。

【００４９】ＭＰＥＧデコード部３２は、復号部３１によって復号（解読）された符号化されているコンテンツデータを受け取り、ＭＰＥＧ方式で符号化されているその復号（解読）されたコンテンツデータを復号し、この復号されたコンテンツデータをモニタ３に供給する（図５のDecode）。そして、モニタ３は、このコンテンツデータを再生画像として図示しない表示画面に表示する。

【００５０】上述したように、第１の実施の形態においては、公開鍵を使用し、この公開鍵をディスクに記録しておくと、公開鍵の配布が容易となる。また、公開鍵を複数記録しておけば、ＭＰＥＧデコーダボード１２の製造者（ボードメーカー）に秘密鍵を配布するとき、ボードメーカー毎に異なる鍵を割り当てることができる。よって、１つのボードメーカーの秘密鍵が破られた場合でも、他のボードメーカーには別の秘密鍵が割り当てられているため、他のボードメーカーの秘密鍵はそのまま使用でき、被害を最小限に食い止めることができる。

【００５１】さらに、ディスクドライブ１１において、秘密鍵ｎはもとより、公開鍵α，β，ｐを保持しておく必要がないので、ディスクドライブにおける管理が容易となる。

【００５２】なお、ディスクドライブ内の制御部２０は、暗号化部２２と一体化して構成してもよい。また、ＭＰＥＧデコーダボード内の制御部３０は、復号部３１と一体化して構成してもよい。

【００５３】また、以上の第１の実施の形態においては、ＭＰＥＧデコーダボード１２からＩＤをディスクドライブ１１に供給し、ディスクドライブ１１において認証を行うようにしたが、ディスクドライブ１１からＩＤを供給し、ＭＰＥＧデコーダボード１２において認証を行うようにしてもよい。また、ディスクとして、ＤＶＤ－ＲＯＭを用いる場合を例としたが、本発明は、その他の記録媒体に記録されているデータを再生する場合にも適用することができる。なお、ディスクがＲＡＭタイプのディスクである場合、制御部２０は、所定の指令が入力されたとき、そのフラグを無効なフラグに書き換えることも可能である。

【００５４】図６は、以上の第１の実施の形態におけるＤＶＤ－ＲＯＭ２に対してデータを記録する記録装置の構成例を示している。図６に示すように、合成部５１は、ＩＤ供給源４１からのＩＤ、フラグ供給源４２からのフラグ、および公開鍵供給源４３からの公開鍵α，β，ｐをキーテーブル（Key Table）のデータとして合成し、その合成されたデータを合成部５２に供給する。また、コンテンツデータ供給源４４からのビデオデデータ等のコンテンツデータ（Contents）がＭＰＥＧエンコード部５３に供給され、ＭＰＥＧエンコード部５３は、コンテンツデータをＭＰＥＧ方式に従って符号化し、符号化されたコンテンツデータを合成部５２に供給する。合成部５２は、合成部５１より入力されたキーテーブルのデータと、ＭＰＥＧエンコード部５３からの符号化されたコンテンツデータを合成して、記録データとして出力する。そして、この記録データが原盤５４に記録される。さらに、その原盤５４から大量のレプリカとしての

ＤＶＤ－ＲＯＭ２が生成される。これにより、ＤＶＤ－ＲＯＭ２には、コンテンツデータの他、各ＩＤに対応したフラグ及び公開鍵からなるキーテーブルが記録される。

【００５５】次に、本発明を適用した第２の実施の形態について説明する。なお、第２の実施の形態を説明するにあたり、まず、コンテンツデータをＤＶＤ—ＲＯＭに記録する記録装置を説明した後、パーソナルコンピュータの構成を説明する。

【００５６】図７は、第２の実施の形態におけるＤＶＤ－ＲＯＭ７２に対してデータを記録する記録装置の構成例を示している。この第２の実施の形態においては、コンテンツデータが暗号化され、暗号化コンテンツデータがＤＶＤ－ＲＯＭ７２に記録されるようになされている。

【００５７】コンテンツ情報源６１からのコンテンツデータは、ＭＰＥＧエンコード部６９に供給される。ＭＰＥＧエンコード部６９は、コンテンツデータをＭＰＥＧ方式に従って符号化し、符号化コンテンツデータを暗号化部６２に供給する。また、暗号化鍵供給源６３からの暗号化鍵Ｑが暗号化部６２に供給される。暗号化部６２は、暗号化鍵Ｑを用いて、例えば、符号化コンテンツデータをＤＥＳ（Data Encryption Standard）方式に従って暗号化し、暗号化コンテンツデータを合成部７０に供給する。

【００５８】一方、この暗号化鍵Ｑは、暗号化鍵暗号化部６４にも供給される。また、公開鍵供給源６７からの公開鍵α，β，ｐが暗号化鍵暗号化部６４に供給され、暗号化鍵暗号化部６４は、次式（８）及び（９）に従って、公開鍵α，β，ｐを用いて、暗号化鍵Ｑを暗号化し、暗号化された暗号化鍵ｘ，ｙを生成する。

$x = \alpha^{k3} \bmod (p)$　…（８）

$y = Q \cdot \beta^{k3} \bmod (p)$　…（９）

ここで、ｋ３は、適宜選択されるランダムな番号（値）である。

【００５９】また、合成部６８は、ＩＤ供給源６５からのＩＤ、フラグ供給源６６からのフラグ、公開鍵供給源６７からの公開鍵α，β，ｐ、並びに暗号化部６４からの暗号化された暗号化鍵ｘ，ｙを合成し、キーテーブルとして合成部７０に供給する。合成部７０は、合成部６８から供給されたキーテーブルのデータと、暗号化部６２からの暗号化コンテンツデータを合成して、記録データとして出力する。そして、この記録データが原盤７１に記録される。さらに、その原盤７１から大量のレプリカとしてのＤＶＤ－ＲＯＭ７２が製造される。これにより、図７に示すように、ＤＶＤ－ＲＯＭ７２には、暗号化コンテンツデータの他に、各ＩＤに対応したフラグ、公開鍵ｋｅｙｉ（αｉ，βｉ，ｐｉ）、並びに暗号化された暗号化鍵（ｘｉ，ｙｉ）が、キーテーブルとして記録される。

【００６０】次に、上述したような方法で製造されたＤＶＤ－ＲＯＭ７２に記録されているデータを再生する第２の実施の形態のパーソナルコンピュータの構成について説明する。図８は、本発明を適用した第２の実施の形態のパーソナルコンピュータの構成例を示している。パーソナルコンピュータ８０は、ＤＶＤ—ＲＯＭ７２をドライブするディスクドライブ８１と、ディスクドライブ８１によって再生された再生データが供給され、この再生データをデコードするＭＰＥＧデコーダボード８２から構成されている。ＭＰＥＧデコーダボード８２からの復号されたコンテンツデータは、モニタ７３に供給され、モニタ７３は、図示しない表示画面に再生画像を表示するようになされている。この場合におけるディスクドライブ８１とＭＰＥＧデコーダボード８２の構成は、基本的に図１に示す場合と同様である。

【００６１】ディスクドライブ８１は、ＤＶＤ－ＲＯＭ７２を駆動し、所定のアクセス点にアクセスして、そこに記録されているデータを再生する駆動部９１、駆動部９１から再生データを暗号化し、その暗号化データを出力する暗号化部９２、及び駆動部９１と暗号化部９２を制御する制御部９０から構成されている。ＤＶＤ－ＲＯＭ７２には、所定の位置（例えば最内周トラック）に、暗号化に使用される公開鍵α、β、ｐ及び暗号化された暗号化鍵ｘ，ｙを含むキーテーブルのデータが予め記録されている。なお、ＤＶＤ－ＲＯＭ７２に記憶されているコンテンツデータは、ＭＰＥＧ方式によって符号化されているデータである。

【００６２】また、ＭＰＥＧデコーダボード８２は、第１の実施の形態と同様に、パーソナルコンピュータ８０に対して、適宜装着されるボードであって、暗号化部９２より供給される暗号化データを復号（解読）し、その復号（解読）された暗号化コンテンツデータを出力する復号部１０１を有している。この復号部１０１は、復号（解読）処理を行うために必要な秘密鍵ｎと、MPEGデコーダボード８２を識別するＩＤを記憶するメモリ１０３を有している。

【００６３】復号部１０１から出力された復号された暗号化コンテンツデータは、復号部１０４に供給される。また、暗号化鍵復号部１０５は、ディスクドライブ８１の駆動部９１からの暗号化された暗号化鍵ｘ，ｙを受け取り、秘密鍵ｎと公開鍵ｐを用いてこの暗号化鍵Ｑを復号（解読）し、この復号された暗号化鍵Ｑを復号鍵として復号部１０４に供給する。そして復号部１０４は、この復号鍵を用いて暗号化コンテンツデータを復号（解読）し、復号（解読）された符号化コンテンツデータは、ＭＰＥＧデコード部１０２に供給され、ＭＰＥＧ方式によって復号され、コンテンツデータとして出力されるようになされている。制御部１００は、復号部１０１、ＭＰＥＧデコーダ部１０２、復号部１０４及び暗号化鍵復号部１０５を制御する。

【００６４】次に、図９と図１０のフローチャート、図１１のタイミングチャート、及び図１２の模式図を参照して、その動作について説明する。図９は、図８のディスクドライブ８１の処理を説明するフローチャートであり、図１０は、図８のＭＰＥＧデコーダボード８２の動作を説明するフローチャートである。また、図１１のタイミングチャートは、ディスクドライブ８１とＭＰＥＧデコーダボード８２との間において授受されるデータと、各データに対応して実行される演算を表している。さらに、図１２は、ディスクドライブ８１とＭＰＥＧデコーダボード８２との間のデータの流れを示すための模式図である。

【００６５】ＤＶＤ－ＲＯＭ７２に記録されているデータを再生する場合、最初に図１０のステップＳ５１において、ＭＰＥＧデコーダボード８２の制御部１００は、ＭＰＥＧデコーダボードの識別データとしてのＩＤを復号部１０１のメモリ１０３から読み出し、ディスクドライブ８１の制御部９０に送信する。このＩＤは、図１１に示すように、Request Challenge（ＩＤ）としてディスクドライブ８１に送られる。

【００６６】ディスクドライブ８１の制御部９０は、ＭＰＥＧデコーダボード８２の制御部１００から送られてきたＩＤを図９のステップＳ３１において受け取る。そして、制御部９０はステップＳ３２に進み、ステップＳ３１で受け取ったＩＤに対応する公開鍵を、ＤＶＤ－ＲＯＭ７２から読み取るように、駆動部９１を制御する。

【００６７】すなわち、図１２に模式的に示されるように、ＤＶＤ－ＲＯＭ７２の所定のトラックには、キーテーブルとして、コンテンツデータを暗号化した暗号化鍵Ｑを公開鍵を用いて暗号化した暗号化された暗号化鍵ｘ，ｙと、このＤＶＤ－ＲＯＭ７２を再生して得られるＭＰＥＧ方式によって符号化されているコンテンツデータを暗号化する公開鍵（public key）とが、各公開鍵（ｋｅｙ１，ｋｅｙ２，ｋｅｙ３，……）及び暗号化された暗号化鍵（（ｘ１，ｙ１），（ｘ２，ｙ２），（ｘ３，ｙ３）……）が有効であるか否かを表すフラグと共に記録されている。

【００６８】図１２において、有効な公開鍵（ｋｅｙ１，ｋｅｙ２）及び暗号化された暗号化鍵（（ｘ１，ｙ１），（ｘ２，ｙ２））は○印を付して表し、無効な公開鍵（ｋｅｙ３）及び暗号化された暗号化鍵（ｘ３，ｙ３）は×印を付して表している。ＤＶＤ－ＲＯＭ７２を初めて製造したとき、全ての公開鍵及び暗号化鍵Ｑは有効とされている。しかしながら、例えば、公開鍵及び暗号化鍵Ｑの中の所定のもの（図１２の第２の実施の形態の場合、ｋｅｙ３及び（ｘ３，ｙ３）に対応する暗号化鍵Ｑ）が第３者に破られしまったような場合、その公開鍵及び暗号化鍵Ｑに対応するフラグは無効として記録される。

【００６９】なお、各公開鍵ｋｅｙ１，ｋｅｙ２，ｋｅｙ３，……は、それぞれ公開鍵（α１，β１，ｐ１），（α２，β２，ｐ２），（α３，β３，ｐ３），……で構成されている。

【００７０】このような公開鍵、暗号化された暗号化鍵Ｑ及び有効フラグを表すキーテーブルが、ＤＶＤ－ＲＯＭ７２のＲＯＭ領域に記録されている場合には、このデータを書き換えることができないため、新しいバージョンのディスクとして、実質的に同一のコンテンツデータが記録されているディスクを新たに製造するときに、キーテーブルの有効フラグだけが書き換えられる。

【００７１】制御部９０は、駆動部９１を制御し、駆動部９１は、ＤＶＤ－ＲＯＭ７２の所定のトラックに記録されているキーテーブルを読み出す。そして、この読み出したキーテーブルは制御部９０に供給され、制御部９０は、この読み出されたキーテーブルから、ステップＳ３１で受け取ったＩＤに対応する公開鍵、暗号化された暗号化鍵及びそれらに対応するフラグを検出する。換言すれば、ＭＰＥＧデコーダボード８２の正規の製造者（ボードメーカー）に対してはＩＤが予め与えられており、ＤＶＤ－ＲＯＭ７２の製造者は、各ＩＤに対応する公開鍵及び暗号化鍵Ｑを選定して、その公開鍵と公開鍵によって暗号化された暗号化鍵ｘ，ｙをテーブルに記憶しておく。そこで、このステップＳ３２で、各ＩＤに対応する公開鍵及び暗号化された暗号化鍵ｘ，ｙが検出される。

【００７２】さらに、ステップＳ３３において、この公開鍵及び暗号化された暗号化鍵に対応するフラグが有効とされているか否かを判定する。上述したように、例えば、不正コピーを行っているＭＰＥＧデコーダボード８２の製造者（ボードメーカー）に割り当てられいるＩＤが発見された場合においては、そのＩＤに対応する公開鍵は無効とされる。そして、その発見後に製造されるＤＶＤ－ＲＯＭ７２に対応する公開鍵及び暗号化鍵Ｑを無効とするフラグが記録される。ステップＳ３１で受け取ったＩＤに対応する公開鍵が無効と判定された場合、処理が終了される。すなわち、この場合においては、ＭＰＥＧデコーダボード８２は、ＤＶＤ－ＲＯＭ７２の再生データを受け取ることができないことになる。なお、ここまでのデータの授受の流れが、図１２に示されるKey exchangeに対応している。

【００７３】一方、ステップ３３において、ステップ３１で受け取ったＩＤに対応する公開鍵が有効であると判定された場合、ステップＳ３４に進み、制御部９０は、第１に実施の形態と同様に、上述した式（１）からChallenge（Ｃ）を計算し、ＭＰＥＧデコーダボード８２の制御部１００に供給する。

【００７４】図１２に示すように、このようにして計算されたChallenge（Ｃ）は、ＭＰＥＧデコーダボード８２の制御部１００に供給される。制御部１００は、図１０のステップＳ５２において、このChallenge（Ｃ）を

受け取る。そして、制御部１００は、ステップＳ５３に進み、第１の実施の形態と同様に、所定のランダムな番号ｋ２を選択し、上述した式（２）、（３）からデジタルシグニチャｒ，ｄを演算し、その結果をResponse（ｒ，ｄ）として、ディスクドライブ８１に供給する。

【００７５】図１１に示すように、上述した式（２）及び（３）から求められたデジタルシグニチャｒ，ｄは、Response（ｒ，ｄ）として、ディスクドライブ８１の制御回路９０に供給される。制御部９０は、図９のステップＳ３５において、このResponse（ｒ，ｄ）を受け取り、ステップＳ３６に進み、ステップ３６において、このResponse（ｒ，ｄ）内のデジタルシグニチャｒ，ｄをチェックする。

【００７６】すなわち、制御部９０は、図１２に示すように、βｒ・ｒｄを演算するとともに、αＣ mod （ｐ）を演算し、両者の値が等しいか否かを判定する。ＭＰＥＧデコーダボード８２が、正規のデコーダである場合、第１の実施の形態と同様に、デジタルシグニチャｒ，ｄと公開鍵βとを用いて演算される値βｒ・ｒｄの値は、Challenge（Ｃ）、公開鍵α，ｐを用いて求められる値αＣ mod（ｐ）の値と等しくなる。逆に、ＭＰＥＧデコーダボード１２が正規のデコーダではない場合、両者の値は異なるものとなる。この場合、制御部９０の処理は終了される。従って、この場合、ＤＶＤ－ＲＯＭ７２のビデオデータはＭＰＥＧデコーダボード８２に出力されないことになる。

【００７７】ステップＳ３６において、演算された２つの値が等しいと判定された場合、ステップＳ３７に進み、制御部９０は、第１の実施の形態と同様に、Session KeyＳを上述した式（４）より演算する（図１２のSession Key S）。

【００７８】一方、ＭＰＥＧデコーダボード８２の制御部９０は、図１０のステップＳ５３において、Response（ｒ，ｄ）を計算して、ディスクドライブ８１に供給した後、ステップＳ５４に進み、第１の実施の形態と同様に、ステップＳ５２で受け取ったChallenge（Ｃ）を用いて上述した式（５）に従って、Session Key Ｓ’を演算する（図１２のSession Key S*）。

【００７９】よって、ステップＳ３７においてディスクドライブ８１の制御部９０によって計算されたSession Key Ｓと、ステップＳ５４においてＭＰＥＧデコーダボード８２の制御部１００によって演算されたSession Key Ｓ’は、第１の実施の形態で説明したように、それぞれ上述した式（６）及び（７）で表され、両者は等しい値となる。すなわち、ディスクドライブ８１とＭＰＥＧデコーダボード８２において、それぞれ同一の暗号化鍵が得られたことになる。

【００８０】さらに、ディスクドライブ１１において、Session Key Ｓを演算すると、ステップＳ３８に進み、駆動部９１は、ＤＶＤ－ＲＯＭ７２より再生された暗号化された暗号化鍵ｘ，ｙを、そのままＭＰＥＧデコーダボード８２に供給する（図１２のｘ，ｙ（as is））。

【００８１】ＭＰＥＧデコーダボード８２の制御部１００は、Session KeyＳ’が得られたら、次にステップＳ５５に進み、ステップ３８において、暗号化鍵復号部１０５がディスクドライブ８１か供給された暗号化された暗号化鍵ｘ，ｙを受け取るように制御し、また、メモリ１０３から秘密鍵ｎを読み出して、暗号化鍵復号部１０５に供給し、次に、ステップＳ５６に進む。ステップ５６において、暗号化鍵復号部１０５は、暗号化された暗号化鍵ｘ，ｙを次式（１０）に従って復号（解読）し、この復号された暗号化鍵Ｑ（復号鍵）が復号部１０４に供給される（図１２のKey Decryption）。

Ｑ＝（ｙ／ｘｎ） ｍｏｄ（ｐ） …（１０）

【００８２】すなわち、暗号化鍵復号部１０５は、秘密鍵ｎと公開鍵ｐを用いて、暗号化されたｘ，ｙから暗号化鍵Ｑを復号（解読）する。

【００８３】一方、ディスクドライブ８１は、ステップＳ３８で暗号化された暗号化鍵ｘ，ｙをＭＰＥＧデコーダボード８２に供給した後、さらに、ステップＳ３９に進み、制御部９０は、駆動部９１を制御して、駆動部９１は、ＤＶＤ－ＲＯＭ７２から暗号化コンテンツデータを再生し、その再生された暗号化コンテンツデータ（暗号化鍵Ｑで暗号化されているコンテンツ）を暗号部９２に供給するとともに、制御部９０は、ステップＳ３７で求めたSession Key Ｓを暗号化部９２に供給する。暗号化部９２は、再生された暗号化コンテンツデータをSession Key Ｓで暗号化して、暗号化データをＭＰＥＧデコーダボード８２に供給する（図１２のEncryption）。

【００８４】ＭＰＥＧデコーダボード８２の復号部１０１は、図１０のステップＳ５５において、暗号化部９２から供給された暗号化データを受け取り、ステップＳ５６において、その暗号化データを、ステップＳ５４で求めたSession Key Ｓ’を用いて復号（解読）する（図１２のDecryption）。上述したように、Session Key Ｓ’は、Session Key Ｓと同一の値であるので、正しい復号（暗号の解読）を行うことができる。これにより、Session Key Ｓによる暗号化が解除され、暗号化鍵Ｑで暗号化されている暗号化コンテンツデータが得られることになる。そして、この暗号化コンテンツデータが復号部１０４に供給される。

【００８５】次にステップＳ５９に進み、復号部１０４は、復号部１０１からの暗号化コンテンツデータを復号部１０４からの復号（解読）された暗号化鍵Ｑ（復号鍵）を用いて復号（解読）する。すなわち、第２の実施の形態の場合、ＤＥＳの復号処理が実行される（図１２のDecryption）。そして、この復号（解読）された符号化されているコンテンツデータ（符号化コンテンツデータ）がＭＰＥＧデコード部１０２に供給される。

【００８６】ＭＰＥＧデコード部１０２は、復号部１０

４によって復号（解読）された符号化コンテンツデータを受け取り、この符号化コンテンツデータをＭＰＥＧ方式で復号し、この復号されたコンテンツデータをモニタ３に供給する（図１２のDecode）。そして、モニタ７３は、このコンテンツデータを再生画像として図示しない表示画面に表示する。

【００８７】以上、上述したように、第２の実施の形態においては、ディスクに記録されているコンテンツデータが暗号化されており、さらに、ディスクドライブ８１において、このコンテンツデータが暗号化される（つまり、コンテンツデータが２重に暗号かされている）ため、ディスクドライブ８１とＭＰＥＧデコーダボード８２間のデータを傍受したとしても、第１の実施の形態の効果に比べて、不正コピーはより困難になる。

【００８８】また、このように、この第２の実施の形態においては、セッションキーＳを求めるとき用いられる公開鍵α，ｐと、認証処理（識別処理）を行うとき用いられる公開鍵βとを用いて、コンテンツを暗号化する暗号化鍵Ｑを暗号化するようにしたので、暗号化のために必要となる鍵の数を減らすことができる。すなわち、暗号化鍵Ｑを、公開鍵α，β，ｐ以外の鍵を用いて暗号化することも可能であるが、そのようにすると鍵の数が増加し、鍵が破られた場合において、鍵を変更する（無効とする）処理が困難になる。そこで、この第２の実施の形態のように、セッションキーＳと認証に用いられる公開鍵α，β，ｐを、コンテンツを暗号化する暗号化鍵Ｑの暗号化にも共通に用いるようにすることにより、鍵の数を減らすことができる。

【００８９】また、第２に実施の形態において、ディスクドライブ内の制御部９０は、暗号化部９２と一体化して構成してもよい。また、ＭＰＥＧデコーダボード内の制御部１００は、復号部１０１、１０４及び１０５と一体化して構成してもよい。

【００９０】さらに、第２の実施の形態においては、ＭＰＥＧデコーダボード８２からＩＤをディスクドライブ８１に供給し、ディスクドライブ８１において認証を行うようにしたが、ディスクドライブ８１からＩＤを供給し、ＭＰＥＧデコーダボード８２において認証を行うようにしてもよい。また、ディスクとして、ＤＶＤ－ＲＯＭを用いる場合を例としたが、本発明は、その他の記録媒体に記録されているデータを再生する場合にも適用することができる。なお、ディスクがＲＡＭタイプのディスクである場合、制御部９０は、所定の指令が入力されたとき、そのフラグを無効なフラグに書き換えることも可能である。

【００９１】なお、上記第１及び第２の実施の形態においては、図６、図７、図１２に示すように、暗号化された公開鍵ｘ，ｙを、公開鍵α，β，ｐとともにまとめて１つのキーテーブルに登録するようにしたが、例えば図１３に示すように、暗号化された暗号化鍵ｘ，ｙを、フラグとともにＩＤに対応して、公開鍵α，β，ｐのキーテーブルとは別のキーテーブルにまとめるようにすることも可能である。

【００９２】さらに、上記第１及び第２の実施の形態においては、上記した鍵の生成に１方向性関数を用いるようにすることが可能である。この１方向性関数を用いて鍵の生成方法は、本出願人によって、例えば、特願平８－２６９５０２号として先に提案されているものを用いることができる。

【００９３】以上、上記第１及び第２の実施の形態においては、本発明をディスクドライブとデコーダとの間における暗号化鍵の交換と認証を例として説明したが、本発明はこれに限らず、その他の装置に適用することも可能である。例えば、ディスクドライブを、ネットワークを介してデコーダにデータを伝送するセンタに置き換え、センタとデコーダの間において、本発明を適用することもできる。

【００９４】また、上記第１及び第２の実施の形態においては、記録されるコンテンツデータの一例として、ビデオデータを用いて説明しているが、本発明はこれに限らず、オーディオデータ、プログラムデータもしくはその他のデータに適用することが可能である。

【００９５】さらに、上記第１及び第２の実施の形態においては、ＭＰＥＧ方式のエンコーダ及びデコーダを例として説明したが、本発明はこれに限らず、他の符号化方式によるエンコーダ及びデコーダを適用することも可能である。

【００９６】また、本発明の第１及び第２の実施の形態は、ブロック図を用いてハードウェアとして表現しているが、本発明はこれに限らず、ＣＰＵやメモリなどを用いてソフトウェアで実現することも可能である。

【００９７】なお、本発明の主旨を逸脱しない範囲において、さまざまな変形や応用例が考えうる。従って、本発明の要旨は、実施の形態に限定されるものではない。

【００９８】

【発明の効果】以上、上述したように、本発明におけるデータ復号方法およびデータ復号装置によれば、一方は、他方から供給されるデジタルシグニチャｒとランダムな値ｋ１を用いて暗号化鍵を演算し、他方は、チャレンジＣとランダムな値ｋ２を用いて暗号化鍵を演算するようにし、このデジタルシグニチャｒを公開鍵α，ｐとランダムな値ｋ２を用いて演算するようにしたので、暗号化鍵が破られ難くなり、データの不正なコピーを確実に防止することが可能となる。

【００９９】また、本発明における認証方法によれば、デジタルシグニチャｒ，ｄと、所定の公開鍵βとを用いて演算される値と、公開鍵α，ｐとチャレンジＣを用いて演算される値とを比較して、その比較結果に対応して認証を行うようにしたので、より安全な認証システムを構築することが可能となる。

【０１００】さらに、本発明における記録媒体、ディスク製造方法、記録方法及び記録装置によれば、暗号化鍵Ｓを演算するとき用いられる公開鍵α，ｐを、第１の装置または第２の装置を識別する識別データに対応して記録媒体に記録するようにしたので、データの不正なコピーを確実に防止することが可能な記録媒体を実現することができる。

【０１０１】また、本発明における記録媒体、ディスクの製造方法、記録方法及び記録装置によれば、第１の装置または第２の装置を識別するとき用いられる公開鍵βを、識別データに対応して記録媒体に記録するようにしたので、より安全な認証システムを構築することが可能な記録媒体を実現することができる。

【０１０２】さらに、本発明における記録媒体、ディスク製造方法、記録方法及び請求項１８に記載の記録装置によれば、データを暗号化する暗号化鍵Ｑを、暗号化鍵Ｓを演算するとき用いられる公開鍵α，ｐと、第１の装置または第２の装置を識別するとき用いられる公開鍵βとを用いて暗号化した暗号化鍵ｘ，ｙを、第１の装置または第２の装置を識別する識別データに対応して記録するようにしたので、不正なコピーをさらに確実に防止することが可能な記録媒体を実現することができる。

【図面の簡単な説明】

【図１】本発明を適用した第１の実施の形態のパーソナルコンピュータの構成例を示すブロック図である。

【図２】図１のディスクドライブの動作を説明するフローチャートである。

【図３】図１のＭＰＥＧデコーダボードの動作を説明するフローチャートである。

＊【図４】図１の第１の実施の形態の動作を説明するタイミングチャートである。

【図５】図１の第１の実施の形態におけるデータの流れを説明する模式図である。

【図６】本発明を適用したの第１の実施の形態におけるＤＶＤ－ＲＯＭを製造する装置の構成例を示すブロック図である。

【図７】本発明を適用した第２の実施の形態におけるＤＶＤ－ＲＯＭを製造する装置の構成例をすブロック図である。

【図８】本発明を適用した第２の実施の形態のパーソナルコンピュータの構成例を示すブロック図である。

【図９】図８のディスクドライブの動作を説明するフローチャートである。

【図１０】図８のＭＰＥＧデコーダボードの動作を説明するフローチャートである。

【図１１】図８の第２の実施の形態の動作を説明するタイミングチャートである。

【図１２】図８の第２の実施の形態におけるデータの流れを説明する模式図である。

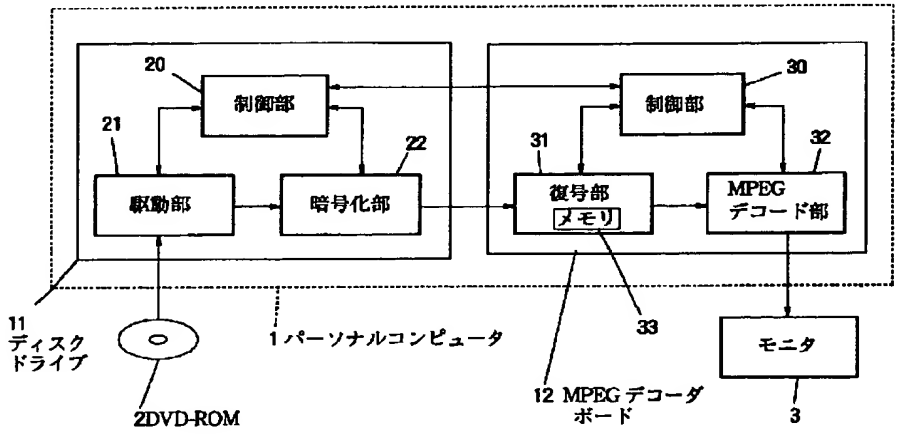
【図１３】コンテンツデータを暗号化した場合のキーテーブルの他の例を示す図である。

【符号の説明】

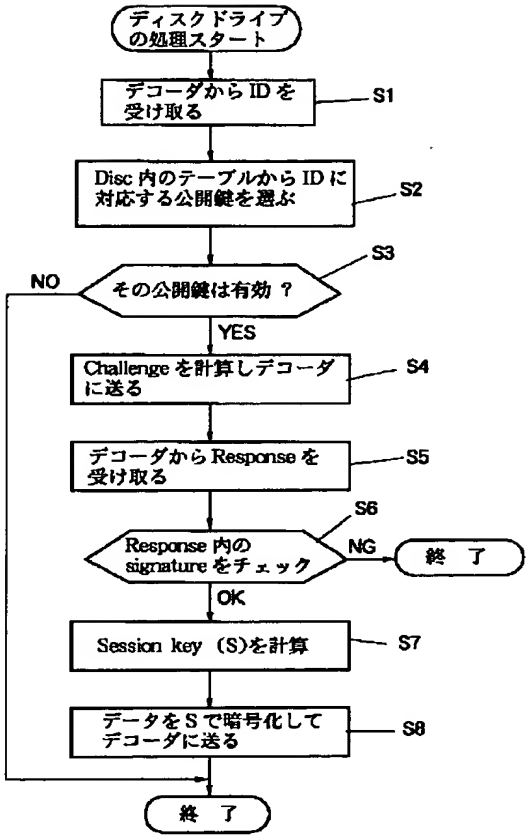
１　パーソナルコンピュータ，　２　ＤＶＤ－ＲＯＭ，　３　モニタ，　１１ディスクドライブ，　１２　ＭＰＥＧデコーダボード，　２０　制御部，　２１　駆動部，　２２　暗号化部，　３０　制御部，　３１　復号部，　３２　ＭＰＥＧデコード部，　３３　メモリ

＊

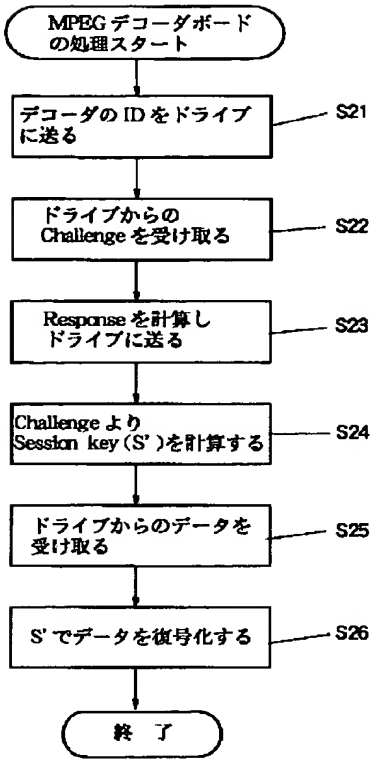
【図１】



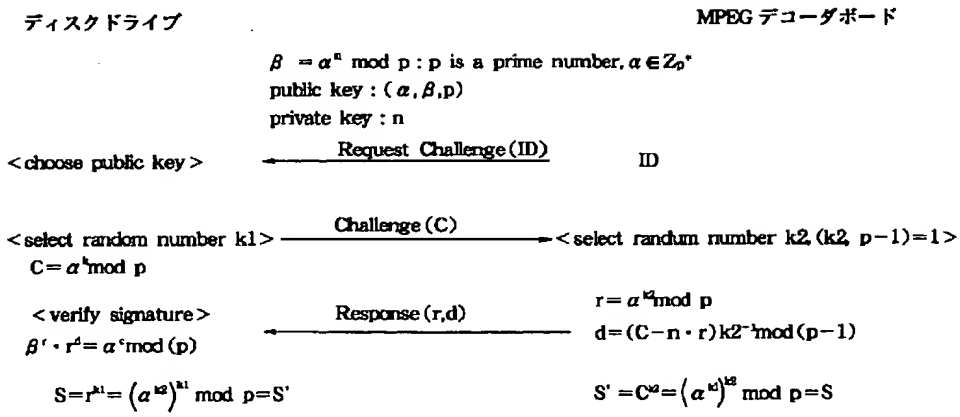
【図２】


ディスクドライブの処理スタート
デコーダからIDを受け取る
S1
Disc内のテーブルからIDに対応する公開鍵を選ぶ
S2
その公開鍵は有効？
S3
NO
YES
Challengeを計算しデコーダに送る
S4
デコーダからResponseを受け取る
S5
Response内のsignatureをチェック
S6
NG
終了
OK
Session key (S)を計算
S7
データをSで暗号化してデコーダに送る
S8
終了

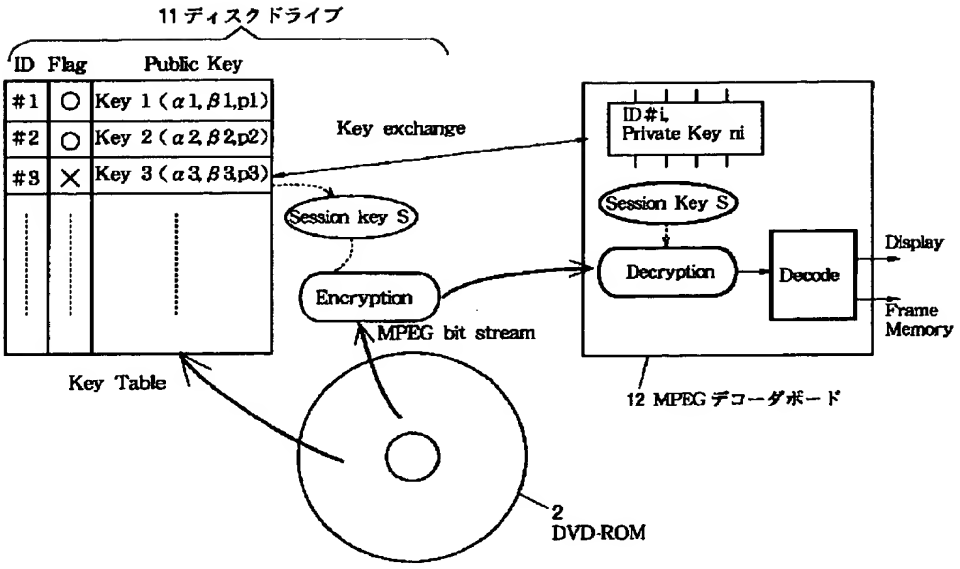
【図３】


MPEGデコーダボードの処理スタート
デコーダのIDをドライブに送る
S21
ドライブからのChallengeを受け取る
S22
Responseを計算しドライブに送る
S23
ChallengeよりSession key (S')を計算する
S24
ドライブからのデータを受け取る
S25
S'でデータを復号化する
S26
終了

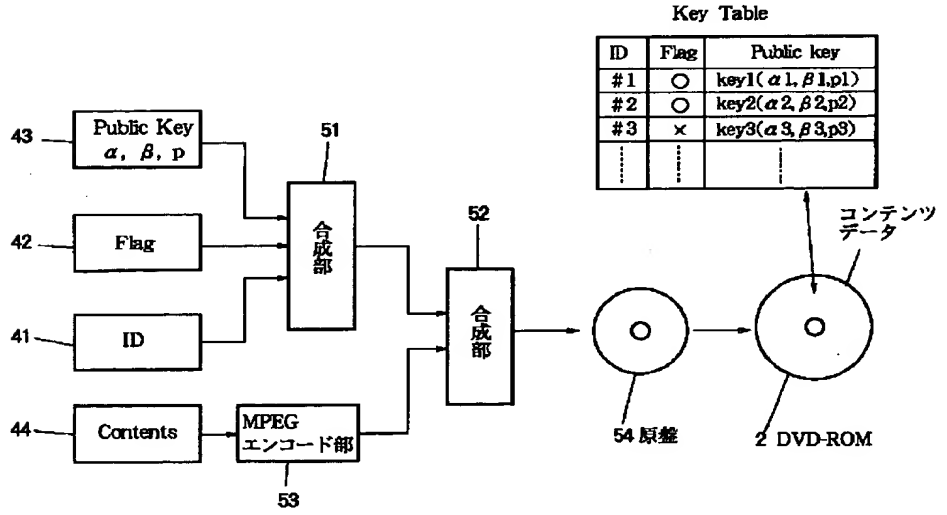
【図４】


ディスクドライブ
MPEGデコーダボード
β = α^n mod p : p is a prime number, α ∈ Zp*
public key : (α, β, p)
private key : n
<choose public key>
Request Challenge (ID)
ID
<select random number k1>
Challenge (C)
<select random number k2, (k2, p−1)=1>
C = α^k1 mod p
<verify signature>
β^r · r^d = α^C mod (p)
Response (r,d)
r = α^k2 mod p
d = (C − n · r) k2^−1 mod (p−1)
S = r^k1 = (α^k2)^k1 mod p = S'
S' = C^k2 = (α^k1)^k2 mod p = S

【図５】



【図６】

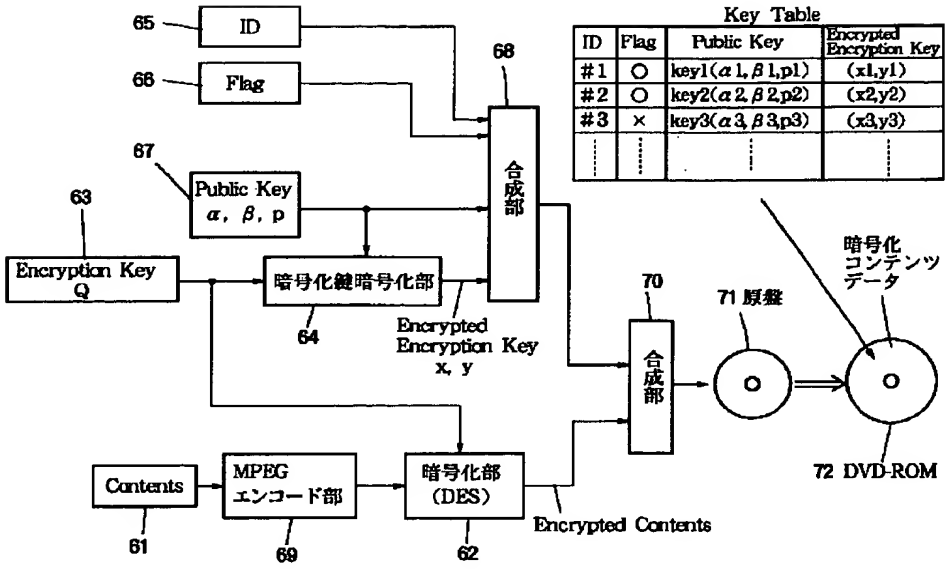


【図１３】

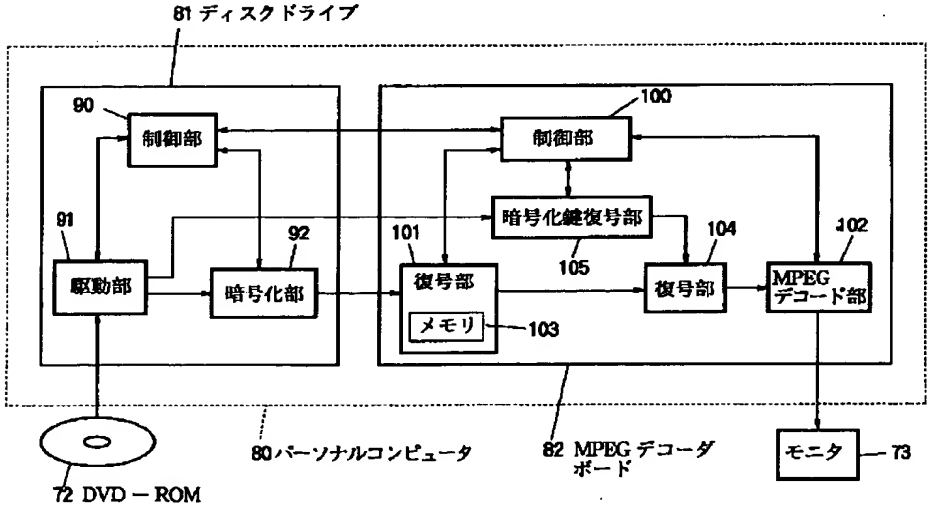
Key Table

ID	Flag	Encrypted Encryption key
#1	○	(x1, y1)
#2	○	(x2, y2)
#3	×	(x3, y3)
⋮	⋮	⋮

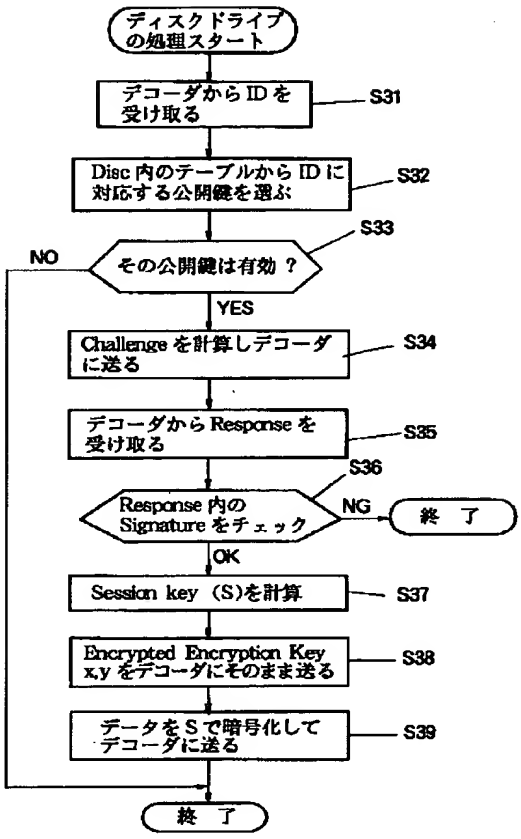
【図７】


65
ID
66
Flag
67
Public Key
α, β, p
63
Encryption Key
Q
暗号化鍵暗号化部
64
68
合成部
Encrypted
Encryption Key
x, y
Key Table
ID
Flag
Public Key
Encrypted Encryption Key
#1
O
key1(α1,β1,p1)
(x1,y1)
#2
O
key2(α2,β2,p2)
(x2,y2)
#3
×
key3(α3,β3,p3)
(x3,y3)
70
合成部
71 原盤
暗号化
コンテンツ
データ
72 DVD-ROM
Contents
61
MPEG
エンコード部
69
暗号化部
(DES)
62
Encrypted Contents

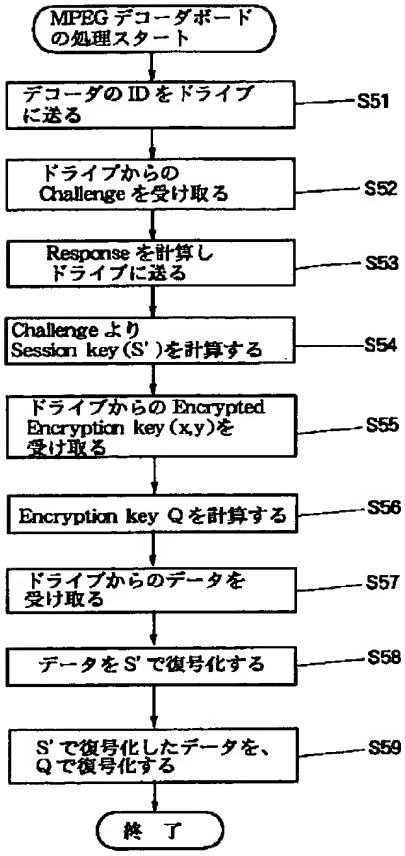
【図８】


81 ディスクドライブ
90
制御部
91
駆動部
92
暗号化部
100
制御部
暗号化鍵復号部
101
復号部
メモリ
103
105
104
復号部
102
MPEG
デコード部
72 DVD－ROM
80 パーソナルコンピュータ
82 MPEG デコーダ
ボード
モニタ
73

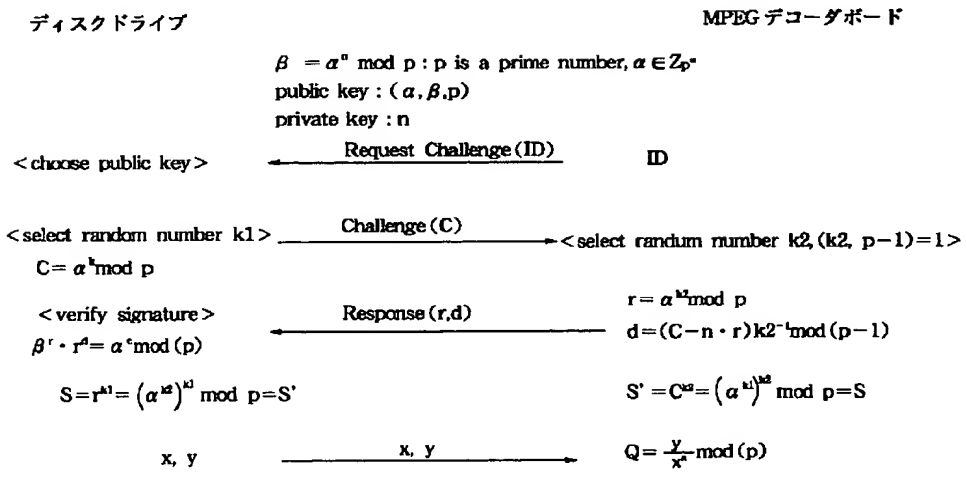
【図９】


ディスクドライブの処理スタート
デコーダからIDを受け取る
S31
Disc内のテーブルからIDに対応する公開鍵を選ぶ
S32
S33
その公開鍵は有効？
NO
YES
Challengeを計算しデコーダに送る
S34
デコーダからResponseを受け取る
S35
S36
Response内のSignatureをチェック
NG
終了
OK
Session key (S)を計算
S37
Encrypted Encryption Key x,yをデコーダにそのまま送る
S38
データをSで暗号化してデコーダに送る
S39
終了

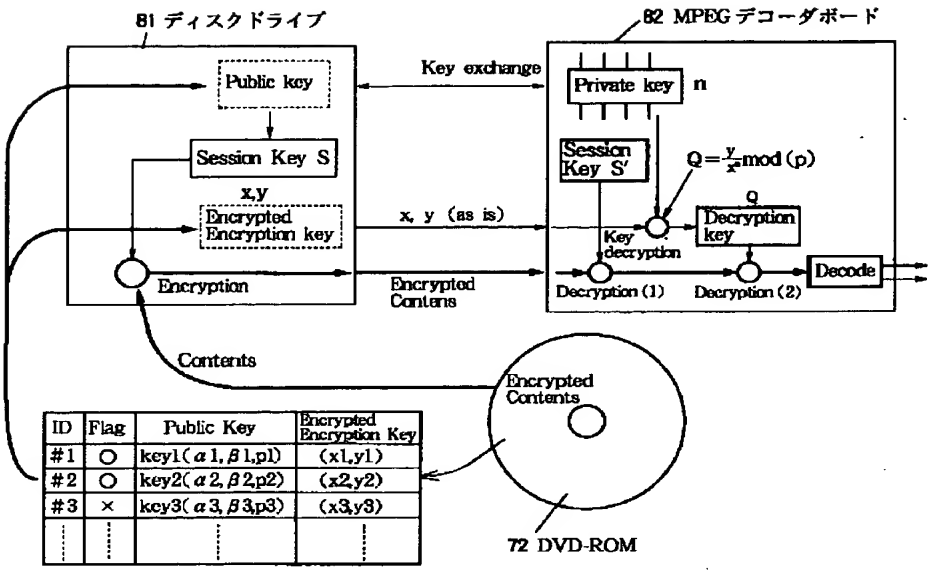
【図１０】


MPEGデコーダボードの処理スタート
デコーダのIDをドライブに送る
S51
ドライブからのChallengeを受け取る
S52
Responseを計算しドライブに送る
S53
Challengeより Session key(S')を計算する
S54
ドライブからのEncrypted Encryption key(x,y)を受け取る
S55
Encryption key Qを計算する
S56
ドライブからのデータを受け取る
S57
データをS'で復号化する
S58
S'で復号化したデータを、Qで復号化する
S59
終了

【図１１】


ディスクドライブ
MPEGデコーダボード
β = α^n mod p : p is a prime number, α ∈ Zp*
public key : (α, β, p)
private key : n
<choose public key>
Request Challenge (ID)
ID
<select random number k1>
Challenge (C)
<select random number k2, (k2, p−1)=1>
C= α^k1 mod p
r= α^k2 mod p
<verify signature>
Response (r,d)
d=(C−n・r)k2^−1 mod (p−1)
β^r・r^d= α^C mod (p)
S=r^k1= (α^k2)^k1 mod p=S'
S' =C^k2= (α^k1)^k2 mod p=S
x, y
x, y
Q= y/x^n mod (p)

【図１２】



ID	Flag	Public Key	Encrypted Encryption Key
#1	○	key1(α1, β1,p1)	(x1,y1)
#2	○	key2(α2, β2,p2)	(x2,y2)
#3	×	key3(α3, β3,p3)	(x3,y3)
⋮	⋮	⋮	⋮

フロントページの続き

(51) Int. Cl.[6]	識別記号	庁内整理番号	F I	技術表示箇所
			Ｈ０４Ｎ　7/13	Ｚ